

# Wireless cracking: there's an app for that

Steve Gold, freelance journalist

Recent advances in the graphics processor power – and software that exploits that processor power – mean that it is now possible to assemble a Windows PC capable of brute force password cracking at speeds of several million attempts every second. And network scanning and cracking tools are now even making it on to smartphones and tablets.

Until quite recently, Russia's Elcomsoft held the 'password recovery' crown in the software stakes, charging clients well into four figures (up to £13,995 for a flagship suite) for the facility. Then in April 2012, a small US start-up called InsidePro quietly upset the applecart with version 2.0 of its software – Extreme GPU Bruteforcer – that is capable, using a high-power graphics card-equipped PC, of cracking a six-character passphrase in under 30 minutes. With a top speed of 450 million password attempts a second, the software sells for just \$39.95 – and there is even a trial version that has all the features of the pay-for edition but is time limited to 180 seconds of operation.

The power of this software has to be seen to be believed – even allowing for all 26 alpha characters in upper and lower case format, plus the 32 special characters in the ASCII character set – it can crunch the near-690 billion required permutations in just 25 minutes, 36 seconds. Let's do the maths:

- Assume the passphrase is six characters long.
- There are 94 possible characters in the password (26 uppercase + 26 lowercase + 32 special + 10 numbers = 94).
- $94 \text{ to the power of } 6 = 689,869,781,056$  unique password permutations.
- $689.87 \text{ billion divided by } 0.45 \text{ (billion passwords/sec)} = 1,533 \text{ seconds} = 25.6 \text{ minutes.}$

The simple process of adding just one or two characters to a passphrase can make it exponentially more secure – moving to seven characters, for example, pushes the time taken to crack a passphrase to a shade over 30 hours,

assuming all permutations are rotated through. Again, let's look at the maths:

- The passphrase is seven characters long.
- There are 94 possible characters in the password.
- $94 \text{ to the power of } 7 = 64,847,759,419,264$  unique password permutations.
- $64,848 \text{ billion divided by } 0.45 \text{ (billion passwords/sec)} = 144,106.67 \text{ seconds} = 2,401 \text{ minutes} = 30.03 \text{ hours.}$

If we add a forced password change to the mix – perhaps every 30 days – and extend the minimum passphrase to 10 characters, with the mandatory inclusion of a mix of alpha plus numeric characters, and at least one special character, we start to approach excellent levels of security.



Steve Gold

## Wireless security

But where does this leave wireless passphrases? And wireless security generally? There are numerous wireless security analysis applications that have been around for several years, available on all the common desktop platforms – Windows, Apple Mac OS X and Linux. Notably, Netstumbler, PRTG Network Monitor and Wireshark are the favoured choice of penetration testers and security analysts everywhere.

But what about the smartphone in your pocket? That Android handset or iPhone has all the key ingredients of a notebook PC – processor, screen, keyboard and wifi functionality – but in a highly portable format. Android wireless analysis apps have been around since almost the beginnings of the portable device operating system, when Google acquired the platform in 2005. Since the arrival of v4.x of the Apple



Figure 1: SubnetInsight in use. The two screenshots to the right show details of a printer.

iPhone and iPad operating system (iOS) in 2011, a number of really powerful wireless analysis apps have started appearing for Apple portable devices. And following the release of iOS 5.x in October 2011 – which was actually released to developers in the late spring of that year – programmers have had access to most of the innermost workings of the iPhone and iPad.

***“Some of the best wireless analysis apps have become extremely popular with black hat and white hat hackers alike and are frequently used by seasoned pen-testers”***

Some of the best wireless analysis apps that are currently available – Shark for Root (Android), SubnetInsight (iOS) and Fing (Android and iOS) – have become extremely popular with black hat and white hat hackers alike and are frequently used by seasoned pen-testers and wireless security researchers.<sup>1,2,3</sup> Shark for Root, for example, sniffs network traffic and writes files capable of being read by Wireshark. At the December 2011 Chaos Computer Club Congress in Berlin, for example, the organisers created a set of smartphone classes for the first time – and given the raft of leading-edge wifi analysis apps that have become available in the past 12 months or so, this is hardly a surprise.

## Sheer pocketability

These wireless smartphone apps are not that functionally different from many desktop and laptop peers. It's true that they do not approach the versatility and complexity of something like Wireshark, but the sheer pocketability of today's handsets makes them a must-have for researchers and ethical hackers in the field. They offer network reconnaissance and enumeration capabilities in a very portable and discreet format. For example, while the suspicions of an IT security manager and/or his staff might be aroused by a site visitor using a high-powered laptop in the firm's coffee lounge to run their network analytics software, hardly



Figure 2: Fing in use.

anyone is going to blink if they see an office visitor in reception ‘checking email’ on a smartphone.

***“The idea that someone could map, attack – and possibly crack open – your corporate network wirelessly, and from inside the building, is all too rarely considered”***

The problem here is that most organisations have spent a small fortune in defending their IT resources from external attack – which is normally defined as IP-based transmissions from outside the company network and firewall. The idea that someone could map, attack – and possibly crack open – your corporate network wirelessly, and from inside the building, is all too rarely considered. And this is before we even start to talk about advanced techniques, such as running a copy of a remote access application such as LogMeIn on a notebook PC in a shoulder bag, and controlling it using an Apple iPhone (the software is free for both devices).

## Public access wireless networks

To put this in context, let's consider how wireless networking is often provisioned. If you're a corporate with visitors to your site, then there's a strong possibility that you have gone to a third-party wifi service provider to support controlled guest access to your company's wireless network.

***“It is usually possible to open up an HTTP session into an IP-connected printer, from where you could – for example – upload a printer firmware update containing malicious code”***

In the UK, one of the biggest providers of these services is The Cloud, which offers controlled – and often free – services to a variety of shopping malls, coffee shops and railway stations across the country, and beyond. The firm also supplies guest services to corporates for a modest monthly fee. In return for a simple site registration, users can access the Internet in a highly controlled fashion. However, the interrogative

smartphone apps mentioned earlier can analyse the wifi router and all devices peered to it without having to log in to the web portal system.

Put simply, this means that before the smartphone user has logged in via the controlled web portal, but after the site software has allocated an IP address to the portable device – and while the user is blocked from accessing the Internet – they can still snoop around on the router's peered IP sessions and, where appropriate, open up an HTTP session into the device concerned. The same effect can be engineered on your home or office wireless router. Portable devices will peer with the router and allow interrogative apps to snoop on the devices that are similarly peered to the unit.

It is usually possible, for example, to open up an HTTP session into an IP-connected printer, from where you could – for example – upload a printer firmware update containing malicious code, allowing Internet users gateway access to the corporate network. If this sounds a little far-fetched, it is worth pointing out that security researcher Ang Cui demonstrated this exact hacking methodology at the 17th Chaos

Computer Club briefings in Berlin at the end of end of 2011.<sup>4</sup>

## Ease of subversion

How easy is it to subvert a wireless network with smartphone and tablet apps? The answer, it has to be said, is ridiculously easy. In a series of tests, we were able to use interrogative wifi apps such as Fing and SubnetInsight to explore devices hooked up to a public access wifi network with ease.

In one session, at a popular major UK shopping mall, for example, we used Network Discovery for Android – which has the advantage of not requiring the tablet/smartphone to be rooted to locate and identify a wifi network. SubnetInsight allowed us to interrogate a fellow shopper's Android handset and access a shop's printer. Opening up an HTTP session to the printer revealed data on the inception of the unit, as well as pages printed. It would also have made it possible, had we wished, to use Cui's 'Print me if you Dare' exploit.

There is also an Android network toolkit known as Anti from an Israeli company called Zimperium, available on free and paid-for versions (an iOS

version is in development for summer 2012 release).<sup>5,6</sup> Anti is interesting from a white hat perspective in that it supports automated tools to carry out penetration testing tasks on insecure wireless networks, running scans to discover open networks, locating devices on those networks and determining vulnerabilities on the peered devices. And once the vulnerabilities have been identified, the app runs exploits from the Metasploit and ExploitDB applications to gain partial or complete access to the device, since they can use the software's brute force password cracking facility – complete with downloadable dictionaries – to gain access.

### ***"DroidSheep allows hijacking of social networking sessions on services such as Facebook and Twitter"***

While even the latest and most powerful dual or quad-core smartphones are limited in processing speeds to under 2GHz, Anti offers users access to pay-per-use gateway applications, allowing smartphone users to leverage Internet-based resources to carry out the serious processing work. Zimperium's cloud-based systems give users seamless access to its servers to complete the wireless cracking process, in return for a modest fee of \$10.00 for 20 exploit analyses or \$50.00 for 200 analyses.

On top of this, if your Android device is rooted, then you can also run an app called DroidSheep. This is named after the FireSheep plug-in for the Firefox browser and, like that tool, it allows hijacking of social networking sessions on services such as Facebook and Twitter.<sup>7</sup> DroidSheep takes the interesting approach of analysing encrypted IP network traffic and looking for patterns that identify SSL-encrypted sessions on sites such as Facebook, Twitter and WordPress, to mention just a few.

## Say hello to your honeypot in your pocket

One pen-testing technique that moves wireless network cracking onto a totally



Figure 3: Zimperium's Anti.



new level is to use a rooted Android device to operate an ad hoc wifi hot spot. While it's possible to use any Android tablet or smartphone running v2.2 of the Android operating system to complete this function, the 'flexibility' of the device is quite limited when it comes to analysis and eavesdropping.

Assuming you have inserted an anonymous pay-as-you-go mobile broadband data SIM into the Android handset, you can then use an app such as Shark for Root that logs all the IP data flowing across the wifi connection to the smartphone's SD card – or memory store in the case of some of the latest Android 4.0 smartphones such as the Samsung Galaxy Nexus.

Creating an ad hoc wireless hotspot on a rooted Android device is a powerful option, since it is possible to site the 'hotspot' in the foyer of a major corporate and 'offer' the same site credentials (eg, SSID) as the company, then wait as staff pass by and their smartphone automatically logs into the more powerful signal offered by your customised Android device. This 'evil twin' technique has been used by pen testers setting up regular – but rogue – wifi routers in offices, but there has so far been relatively little exploration of the potential for doing it with a rooted Android device.

## On the iPhone

While Android may be a distant relative of the Unix/Linux platform, most IT observers view the Apple iPhone and its iOS operating system as a much more secure environment, largely because Apple vets and signs all apps before allowing them to be accessible on the iTunes store. It also rejects apps that provide what the company seems to think are hacking capabilities – even something as apparently benign as wifi signal strength detectors.

Despite this, SubnetInsight – a £2.49 app from Japan's BlueSwine – has been available since July 2011 and has a wealth of interrogative features, including:

- Auto-scan – scans automatically when it gets connected to wifi networks with no user configuration.

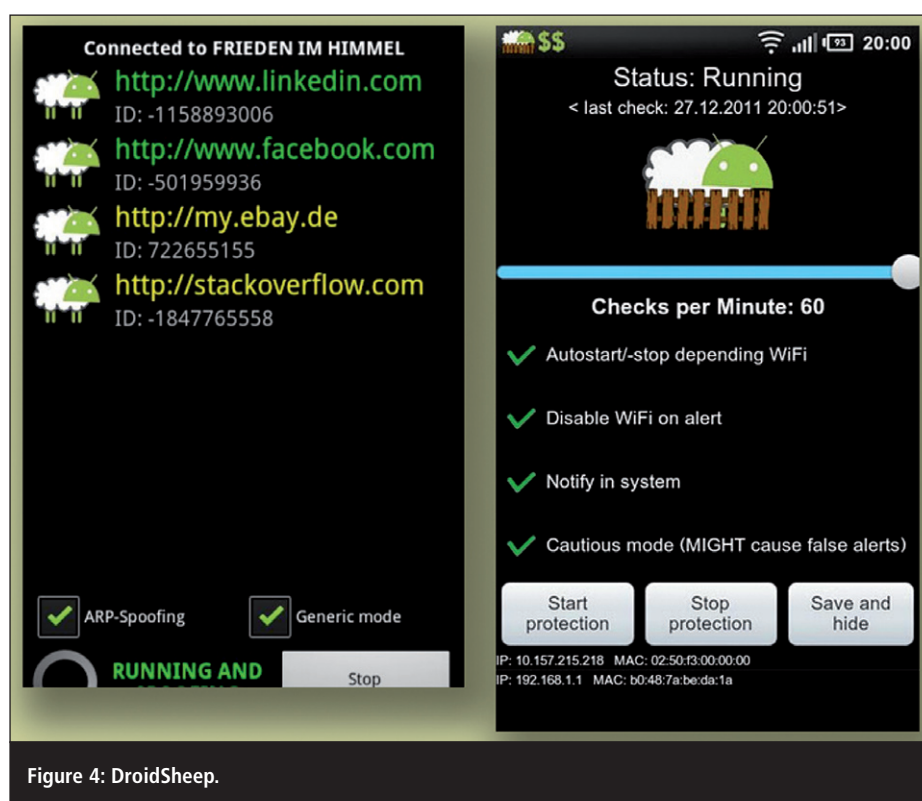


Figure 4: DroidSheep.

- Network logging – manages public IP address and its history, along with geo-location data.
- Powerful host scan – discovers all the hosts in the subnet, including hidden hosts.
- Name resolution – resolves host names via NIC vendor, NetBIOS, Bonjour, MDNS, UPNP and other cloud resources.
- Port scanning – scans all available and known ports for hosts.
- Host fingerprinting – analyses what platform a connected host is running – eg, Windows, Linux/Unix, Mac OS X, mobile device, network printer and VoIP telephony.

The app is popular in Europe, where it has been logged in the iTunes's top 100 charts in several countries (for example, on AppsLists.net) but is not well known in the US and only recently entered the charts for the UK. An 'HD' version is also available for the iPad.

Many researchers prefer Android smartphones for interrogative/pen testing applications because of the ability to root them and side-load apps that simply wouldn't make it through Apple's stringent approval processes. That's why more tools are available on Android. However, apps such as

SubnetInsight and Fing demonstrate how useful even apparently passive iOS devices can be to the researcher or pen tester.

## About the author

*Steve Gold has been a business journalist and technology writer for 26 years. A qualified accountant and former auditor, he has specialised in IT security, business matters, the Internet and communications for most of that time. He also lectures regularly on criminal psychology and cybercrime.*

## References

1. Shark for Root at Google Play. Accessed May 2012. <https://play.google.com/store/apps/details?id=lv.n3o.shark&hl=en>
2. SubnetInsight at iTunes store. Accessed May 2012. <http://itunes.apple.com/gb/app/subnetinsight-scan-manage/id385495647?mt=8>
3. Fing. Overlook Software. Accessed May 2012. [www.overlooksoft.com/](http://www.overlooksoft.com/)
4. Cui, Ang. '28c3: Print Me If You Dare'. Presentation at the 17th Chaos Computer Club Congress, Berlin, 2011. Via YouTube. Accessed May 2012. <https://www.youtube.com/watch?v=njVv7J2azY8>

5. Anti penetration testing tool. Zimperium. Accessed May 2012. [www.zimperium.com/anti.html](http://www.zimperium.com/anti.html).
6. 'Zimperium Finally Releases 'Anti' For Android, Allows You To Use Penetration Testing Tools On The Go'. Android Police, 21 Oct 2011. Accessed May 2012. [www.androidpolice.com/2011/10/03/zimperium-finally-releases-anti-for-android-allows-you-to-use-](http://www.androidpolice.com/2011/10/03/zimperium-finally-releases-anti-for-android-allows-you-to-use-)

[penetration-testing-tools-on-the-go/](http://www.penetration-testing-tools-on-the-go/).

7. DroidSheep. Accessed May 2012. <http://droidsheep.de/>

### Resources

- Morgan, Bradley. 'Wireless Cracking Tools'. WindowSecurity.com, 15 Mar 2006. Accessed May 2012. [www.windowsecurity.com/whitepapers/wireless-cracking-tools.html](http://www.windowsecurity.com/whitepapers/wireless-cracking-tools.html).

- 'How To Crack WEP and WPA Wireless Networks'. Speedguide.net, 21 Nov 2008. Accessed May 2012. [www.speedguide.net/articles/how-to-crack-wep-and-wpa-wireless-networks-2724](http://www.speedguide.net/articles/how-to-crack-wep-and-wpa-wireless-networks-2724).
- 'How to use DroidSheep – tutorial'. YouTube, 9 Sep 2011. Accessed May 2012. <https://www.youtube.com/watch?v=4N-SBx5EF3g>.

# Routing path authentication in link-state routing protocols

Rushdi Hamamreh, Al-Quds University, Jerusalem

**The rapid growth of the Internet has meant that many services are regarded as critical – such as web applications, including email and e-commerce, and real-time applications, such as video conferencing and Voice over IP (VoIP). These rely on the Internet infrastructure to provide them with reliable, efficient and secure communications. However, the routing protocols that the Internet is based on were originally designed to operate in a completely trusted and open environment, assuming no malicious nodes or behaviour. The routing infrastructure was not constructed with security in mind.<sup>1,2</sup> As a result, routers are subject to malicious attacks targeting not only a single subnet or individual users, but also the overall network performance.<sup>3</sup> Therefore the need to secure the Internet has become a significant issue.**

In general, a router is a network device that performs two main functions: it uses routing protocols to build up routing tables and it forwards data packets. Since routers are network-layer devices, faulty or malicious routers can cause malfunctions of the entire routing domain regardless of what services are running within it. Thus, routing attacks can have broad-scale effects since these can deny or reduce communication capabilities.

Attacks on routing protocols can be launched either in the control plane (the part where routers implement the routing protocols to exchange control and update messages that discover the topology and select the shortest paths) or in the data plane – the part where routers forward data along the computed paths.<sup>4</sup>

Many researches have focused on

securing the routing infrastructure by implementing counter-measures in the control-plane phase. However, recent reports suggest that simply protecting the data in the control plane is insufficient to secure routing.<sup>5</sup> An attacker can bypass the control-plane measures and can target the data plane.<sup>6</sup> In the data plane, the most important attack is that a malicious router can forward data along routing paths that are different from the paths that were agreed upon in the control phase, leading to a so-called 'misdirection attack'. Furthermore, an attacker could break into one or more routers, creating an unnoticed disruption by installing Access Control Lists (ACLs) that selectively misdirect data traffic to a path that is not the best or could even be the worst, while keeping the routing pro-

ocols intact and working properly. This leads to harmful consequences, degrading the traffic efficiency of critical applications – including real-time applications that need a good quality-of-service (QoS) – or may cause routing loops. Moreover, a misdirection attack can cause security violations through redirection to a 'black hole', forwarding to a monitoring point or disrupting network usability through a Denial of Service (DoS) attack.

In this article, we focus on a misdirection attack launched in the data-plane phase. We also propose an approach to authenticate the shortest routing path and detect the existence of misconfigured or malicious routers that could misdirect the traffic or incorrectly forward packets within Autonomous Systems (ASs) that apply link-state routing protocols such as Open Shortest Path First (OSPF).<sup>7</sup>

## OSPF overview

OSPF is a widely deployed link-state protocol. Its basic idea can be summarised as follows:

- Each router first discovers its neighbours and the corresponding weights (costs) of their links using Hello the protocol, and then broadcasts this information with reliable Link-State Advertisement (LSA) messages.
- LSAs are refreshed periodically every 30 minutes or on-demand when a